Lesson 8: Compliance Normativa e Privacy

Premessa

L'art. 45 del decreto legge sulle semplificazioni, approvato dal Consiglio dei Ministri, abroga tutte le previsioni contenute nel Codice della privacy e nel Disciplinare tecnico sulle misure di sicurezza che si riferiscono al Documento Programmatico sulla Sicurezza (**DPS**) per il trattamento dei dati personali.

In particolare il decreto interviene all'art. 34, lett. g, comma 1 e comma 1 bis, del D.Lgs 196/2003 (Codice della Privacy) e al suo Allegato B, paragrafi da 19 a 19.8 e 26 (Disciplinare Tecnico in materia di misure minime di sicurezza), **cancellando le norme relative all'obbligo di redazione e aggiornamento del DPS** (sia in forma ordinaria che abbreviata).

Eliminato il DPS, unitamente alle modalità semplificate per la tenuta del DPS, vengono meno anche i relativi riferimenti da riportare all'interno delle relazioni accompagnatorie del bilancio sull'avvenuta redazione o aggiornamento.

Il DPS è un documento che rappresenta la politica adottata del soggetto obbligato per quanto riguarda la privacy.

In altri termini, il documento fotografa la "privacy policy" e sulla base di un'attenta analisi dei rischi procede a definire e programmare le misure necessarie per migliorare la sicurezza del trattamento dei dati personali.

Il DPS doveva essere redatto o aggiornato entro il 31 marzo di ogni anno.

Il soggetto obbligato alla redazione del DPS è il titolare del trattamento dei dati sensibili o giudiziari mediante l'utilizzo di strumenti elettronici, anche attraverso il responsabile, se designato. Il DPS non va inviato al Garante della privacy, ma deve essere conservato presso la propria struttura ed esibito in caso di controllo.

È da sottolineare che il DPS è solo una delle misure minime di sicurezza, **le altre misure previste dal D. Lgs. 196/2003 non vengono abrogate**. Tali misure comportano sanzioni sia di carattere amministrativo che penale e in particolare:

- **Redazione idonee informative** (Art. 13 DLgs 196/2003):
  - Informativa dipendenti e Collaboratori;
  - informativa clienti, fornitori, potenziali clienti, terzi;
  - informativa utenti sito web;
  - informativa candidati all'assunzione;
  - privacy policy sito web.
- **Nomina incaricati al trattamento dati personali** (Art. 30 DLgs 196/2003):
  - redazione documento che individua l'ambito di trattamento dati personali consentito a ciascuna unità organizzativa;
  - redazione lettere d'incarico per ciascun incaricato al trattamento dati personali.
- **Nomina Responsabili al trattamento dati personali e analisi trattamenti affidati in outsourcing** (Art. 29 DLgs 196/2003):
  - redazione lettera di nomina per ciascun Responsabile al trattamento dati personali;
  - analisi dei casi specifici di affidamento dati personali all'esterno dell'Azienda;

- analisi dei flussi di dati intra ed extra Unione Europea;
- individuazione dell'idoneo rapporto da formalizzare con i soggetti esterni ai quali viene affidato il trattamento dati personali.

➢ **Disciplinare interno uso internet e posta elettronica** (Art 154 comma 1 lett. C DLgs 196/2003, Provvedimento Garante 1° Marzo 2007):
- redazione disciplinare interno obbligatorio relativo all'uso di Internet e della posta elettronica.

➢ **Nuove prescrizioni in tema di Amministratori di sistema** (Art 154 comma 1 lett. c) e h) DLgs 196/2003, Provvedimento Garante 27 Novembre 2008):
- adempimenti procedurali e redazione documentazione richiesta dal Provvedimento Generale 27 novembre 2008 – Garante privacy.

➢ **Nuove prescrizioni in materia di videosorveglianza** (Art. 154 comma 1, lett. C DLgs 196/2003, provvedimento garante 8 Aprile 2010):

➢ **Gestione privacy policy sito web, newsletter e servizi interattivi**:
- procedure di gestione dati personali utenti sito web; procedure di attivazione e gestione servizio Newsletter;
- procedure di attivazione e accesso aree riservate.

➢ **Formazione del Personale**.

➢ **Controllo utilizzo della rete e legge contro i crimini informatici** (L.231).

➢ **Gestione e procedure smaltimento o riutilizzo sistemi di rete dismessi o riassegnati** (computer, server etc…).

Con periodicità annuale, il titolare del trattamento **deve aggiornare** il "sistema privacy" in considerazione delle possibili modifiche normative avvenute nel corso dell'anno e **verificare** la rispondenza delle misure adottate riguardanti il trattamento dei dati personali **aggiornando** i documenti e i mansionari adottati.

I titolari devono continuare a mantenersi vigili e organizzati al fine di avere sotto stretto controllo l'effettivo adeguamento della struttura aziendale alla normativa vigente. In quest'ottica l'eliminazione del DPS crea un vuoto nel sistema di sicurezza per il trattamento dei dati posto in essere dall'impresa titolare dello stesso e rende molto più difficoltoso per quest'ultimo dimostrare ciò che è stato fatto in azienda. Stessa cosa per i controlli degli organi di vigilanza che saranno molto meno agevoli in quanto non ci sarà più il documento di riferimento (DPS) attraverso il quale avveniva la verifica della rispondenza alle norme, con particolare riferimento a quanto riguarda l'implementazione delle misure di sicurezza in caso di trattamento dei dati mediante strumenti elettronici.

D'ora in poi, mancando il DPS, gli organi preposti ai controlli (Guardia di Finanza o ispettori dell'Autorità Garante) non potranno più verificare la realtà tramite un documento, ma saranno costretti a fare indagini approfondite per poter accertare l'effettivo rispetto di tutte le misure indicate nel D.Lgs. 196/03, con l'ovvia conseguenza che per l'azienda "verificata" aumenteranno, e di molto, le probabilità che vengano accertate irregolarità e quindi applicate sanzioni.

Durante le lezioni precedenti abbiamo evidenziato come alcuni problemi rilevati possono cagionare danni irreparabili alle organizzazioni aziendali. L'utilizzo di strumenti non idonei possono diventare motivo di denuncia da parte di dipendenti o collaboratori insoddisfatti. Senza il DPS diventa più difficile controllare lo stato di sicurezza raggiunto dal proprio network, ragion per cui un **Audit** che contempli anche i processi aziendali ci può venire in aiuto.

La Normativa Privacy

Le responsabilità

L'art. 15 del D.Lgs. 196/03 stabilisce che "**chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile**". e l'art. 2050 c.c. precisa che "**chiunque cagiona danno ad altri nello svolgimento di una attività pericolosa** [NdR, quale il trattamento dei dati ex art. 15 D.Lgs. 196/03], **per sua natura o per la natura dei mezzi operati, è tenuto al risarcimento, se non prova di aver adottato tutte le misure idonee a evitare il danno**".

Bisogna tenere ben presente che la redazione e l'aggiornamento annuale del DPS sono sempre stati sia un obbligo di legge ma soprattutto lo strumento per il titolare del trattamento, in caso di danni conseguenti al trattamento stesso dei dati, per fornire agevolmente la prova di aver adottato tutte le misure minime e idonee (ex D.Lgs. 196/03) per evitare il danno e pertanto lo strumento per non incorrere nella condanna al risarcimento del danno ai sensi del combinato disposto dell'art. 15 del D.Lgs. 196/03 e dell'art. 2050 c.c.

In altre parole: l'aver abrogato il DPS espone immediatamente i titolari che decidono di non redigere nessun documento, o rinnovare il DPS esistente alla mancanza del miglior strumento aziendale di autoverifica per capire la rispondenza o meno con le prescrizioni della legge in materia di privacy aumentando di fatto il rischio di minor tutela per le persone fisiche (unici soggetti degni di tale tutela per la normativa vigente).
Ma non finisce qui. Infatti la mancanza del DPS espone anche le aziende titolari dei trattamenti ad un rischio in più in quanto si vedono aumentare le possibilità di irregolarità con la normativa vigente che riguarda l'implementazione delle misure tecniche ed organizzative **tuttora obbligatorie** (misure di sicurezza minime e idonee, normativa in materia di amministratori di sistema, obbligo di informativa e raccolta del consenso per il trattamento di dati relativi a persone fisiche) e quindi ……**di subire le relative sanzioni**.
A tale rischio va aggiunta anche la difficoltà oggettiva di non poter fornire la prova. In caso di controlli, ovvero di contenzioso relativo alla richiesta di risarcimento danni legata al trattamento dei dati o a quello di aver adottato tutte le misure minime ed idonee di cui al D.Lgs. 196/03 e all'art. 2050 c.c., non sarà possibile esibire il DPS come prova a Vostro discarico.

Nelle precedenti lezioni abbiamo visto che alcuni strumenti forniti ai dipendenti non sono compliance e cioè con i requisiti minimi di sicurezza, ad esempio protocolli in chiaro implementati nel servizio della posta elettronica. Per questo motivo un dipendente, le cui informazioni viaggiano in chiaro, non può essere responsabile delle informazioni se acquisite da terzi. Ma c'è di più, lo stesso dipendente potrebbe denunciare l'azienda per violazione della privacy.

Le modifiche

Gli interventi modificativi della disciplina in tema di Trattamento dei Dati Personali erano già iniziati con il cosiddetto "Decreto Sviluppo" del Governo Berlusconi (D.L. n. 70/2011) infatti:

- con il provvedimento summenzionato del maggio 2011 era stato abrogato il comma 3-bis dell'art. 5 del D. Lgs. n. 196/03, escludendo così dall'applicazione del codice della privacy il trattamento dei dati personali relativi a persone giuridiche, imprese, enti o

associazioni, ma solo qualora lo stesso fosse effettuato nell'ambito di rapporti intercorrenti esclusivamente tra i medesimi soggetti per le finalità amministrativo-contabili;

- il decreto legge n. 138 del 13.08.2011, recante "Ulteriori riduzioni e semplificazioni degli adempimenti burocratici", aveva dato la facoltà di sostituire il DPS con "**un'autocertificazione** " per i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili e giudiziari quelli relativi ai propri dipendenti e collaboratori, anche se extracomunitari, compresi quelli relativi al coniuge e ai parenti (d.lgs. 196/03, art. 34, co. 1-bis).

Il governo Monti aveva poi proseguito con l'art. 40 del D.L. 6 dicembre 2011 n. 201, contenente le disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici, determinando una piccola "grande rivoluzione" nella disciplina della privacy nel nostro Paese, escludendo dall'applicazione di detta normativa tutti i trattamenti di dati di persone giuridiche, enti e associazioni, pubblici e privati. In pratica, dal dicembre scorso si possono trattare tali dati senza più l'onere di fornire a tali categorie di interessati l'informativa preventiva e senza più dover chiedere il consenso di tali soggetti, nemmeno in caso di trasferimento di dati all'estero.

L'Europa

La normativa in materia di trattamento dei dati personali è in fase di revisione non solo in Italia ma anche negli altri paesi dell'Unione Europea, essendo ormai imminente l'emanazione di un regolamento comunitario che andrà a sostituire la normativa europea di riferimento (la direttiva 95/46 CE del 1995), peraltro con applicazione diretta negli stati membri.
Questo regolamento comunitario è molto importante, perché oltre a uniformare le regole a livello europeo, potrebbe introdurre significative novità quali ad esempio:

- introduzione del principio dell'applicazione del diritto UE anche ai trattamenti di dati personali non svolti nell'UE, se relativi all'offerta di beni o servizi a cittadini UE o tali da consentire il monitoraggio dei comportamenti di cittadini UE;
- introduzione del diritto degli interessati alla "portabilità" del dato oltre che del "diritto all'oblio", fatte salve specifiche esigenze (ad es. per rispettare obblighi di legge, per garantire l'esercizio della libertà di espressione, per consentire la ricerca storica);
- cancellazione dell'obbligo per i titolari di notificare i trattamenti di dati personali, obbligo sostituito da quello di nominare un "data protection officer" (incaricato della protezione dei dati) per tutti i soggetti pubblici e privati al di sopra di un certo numero di dipendenti;
- introduzione del requisito del "privacy impact assessment" (valutazione dell'impatto-privacy) oltre che del principio generale detto "privacy by design" (cioè previsione di misure di protezione dei dati già al momento della progettazione di un prodotto o di un software);
- introduzione dell'obbligo per tutti i titolari di notificare sempre all'autorità competente le violazioni dei dati personali ("personal data breaches") in tempi determinati e molto ristretti (si parla di 48 ore);
- introduzione di poteri più specifici, anche sanzionatori, di requisiti di indipendenza delle autorità nazionali di controllo il cui parere sarà indispensabile qualora si intendano adottare strumenti normativi, comprese leggi, che impattino sulla protezione dei dati personali;

- introduzione dell'obbligo di adozione per le imprese e per gli enti di un vero modello organizzativo per la tutela dei dati, introducendo il principio di responsabilità (accountability), per cui nel caso di controlli saranno loro a dover dimostrare la conformità del proprio operato alle regole comunitarie;

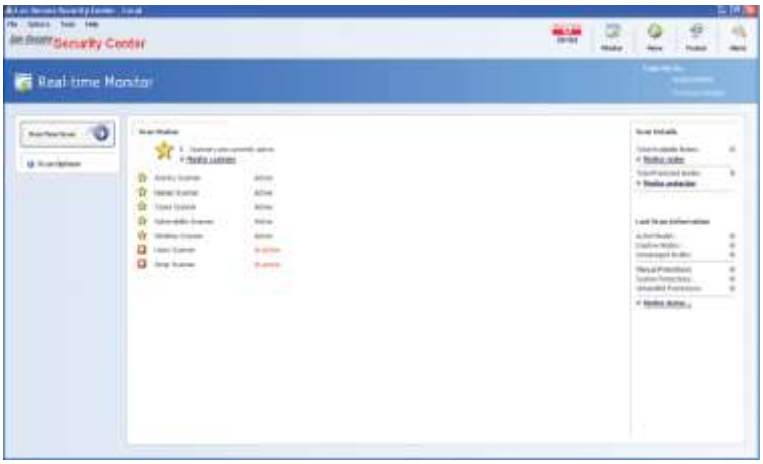
- introduzione di un impianto sanzionatorio di fonte comunitaria, a garanzia dell'efficacia di quanto prescritto, con sanzioni massime previste molto elevate e parametrate al fatturato dell'impresa sanzionata.

Alla luce di quanto sopra, forse gli interventi di "semplificazione" in materia di trattamento di dati personali del Governo Italiano dell'ultimo anno non vanno esattamente nella medesima direzione delle ormai prossime modifiche normative a livello comunitario, modifiche che parrebbero determinare l'introduzione, a breve, di maggiori e più stringenti obblighi in capo ai titolari dei trattamenti.
Si dovrà tuttavia attendere la conversione del D.L. 5/2012 nonché l'approvazione del testo definitivo del nuovo Regolamento UE per avere finalmente una visione complessiva della "nuova" normativa in materia.

Software di gestione e controllo accessi

Security Center

Come evidenziato nelle lezioni precedenti La maggior parte delle minacce si verificano all'interno dell'organizzazione stessa per cui è indispensabile controllare chi si collega alla rete per prevenire quanto previsto dalla 231 contro i crimini informatici.
Security Center è un software per la sicurezza della rete che lavora in "Real Time" in tempo reale. Rileva intrusioni (funzione di IDS e IPS) ed effettua prevenzione proteggendo le rete da potenziali connessioni non autorizzate.



Vediamo insieme cosa è possibile fare:

- bloccare ogni nuovo tentativo di connessione di devices per indirizzo IP, indirizzo MAC o nome macchina, confinandolo in area riservata inviando contestualmente un "alert" all'amministratore di rete;
- settare policy di controllo utente per l'utilizzo dei dispositivi non consentiti. Per esempio l'utilizzo dei sistemi di memoria esterni su porte USB;

- controllare se programmi vitali sono in esecuzione sui client (antivirus e firewall ad esempio);
- confinare una macchina che presenta problemi di elevati broadcast.

Nelle organizzazioni dove chiunque si connette e riceve un indirizzo da server DHCP "Security Center" diventa uno strumento indispensabile per evitare che persone esterne all'organizzazione possano connettersi alla rete arrecando danni.

Conclusioni

Dopo quanto considerato rimane il ragionevole dubbio che il DPS sia stato per anni l'incubo di tante aziende e organizzazioni italiane a tal punto da provare a cassarlo a colpi di decreto.

La bozza infatti indica l'abolizione della lettera h) comma 1 art. 43. Già… ma dell'allegato B non se ne parla. **Quindi?**

Lecito pensare che in caso di dati sensibili permanga comunque l'obbligo.

Ma se viene soppresso il concetto di DPS richiamato anche nelle semplificazioni emanate dal Garante insieme all'autocertificazione e quindi all'impianto della semplificazione stessa……, **come si considera di dover gestire i dati sensibili dei dipendenti?**

Rimettendo in carreggiata il DPS??????

Non è dato sapere.

Ma non è tanto questo il problema.

Qui si sta parlando di sopprimere l'unico strumento di auto-analisi inerente la sicurezza informatica aziendale. Lo stesso strumento che, seppur tanto odiato, ha consentito ad aziende anche di un certo livello, di mantenere nel tempo la propria sicurezza informatica stimolando investimenti che i titolari aziendali, spesso ignari del fatto che l'IT è il fulcro della vita aziendale, hanno accettato solo grazie al pungolo normativo.

Un DPS che, spina nel fianco dei responsabili, ha comunque costretto alla razionalizzazione dei criteri di assegnazione di credenziali piuttosto che alla ristabilizzazione degli idonei livelli di autenticazione secondo il ruolo aziendale, impedendo accessi non dovuti e circolazione di informazioni aziendali non opportune.

Tutti valori scontati oggi, ma assolutamente sottovalutati prima del 2004.

Il DPS è stato bollato da molti come "quel documento terribile e dispersivo", ma in realtà, se ben fatto, ha consentito negli anni di programmare investimenti informatici e far crescere nella mentalità aziende e professionisti. Ora lo si toglie o, per lo meno, lo si riduce solo ai casi di dati sensibili (resterebbe vigente infatti l'Allegato B).

Pienamente d'accordo sulle realtà minime (artigiani, aziende di produzione), ma su soggetti che fanno una ampia gestione anche solo di dati contabili!!! Un'azienda con un milione di dati su persone giuridiche non deve fare il DPS???.

I commenti nella bozza del testo sono:

- ci dobbiamo uniformare alla normativa europea.
- Ok.
- Ma la mentalità italiana in merito al dato trattato, non è quella europea.
- L'italiano parla in ambito aziendale del "suo pc", non del "pc aziendale". Dei "suoi clienti" non dei "clienti della mia azienda".
- La nostra mentalità non è quella europea, **per lo meno non ancora**.

Ci sono aziende dove l'obbligo del DPS ha costretto alla mappatura di server, di trattamenti, di

soggetti autorizzati ad accedere ai dati e ai relativi livelli di visualizzazione.

Noi suggeriamo di utilizzare l'**Audit** in ambito di **Network Assessment** quale sostituto del **DPS** redigendo un documento di programmazione e autoanalisi, atto a far rilevare vulnerabilità e a programmare miglioramenti.

Nel frattempo prova a scaricare il trial di "Security Center" e a vedere quanto e come ti può aiutare nella pianificazione del tuo lavoro e nella prevenzione relativa alla sicurezza della tua rete.

Il Tuo
EterNet Team